EMSD Technology Conference
CxP Software Topics

EMSD Technology Exchange
Software Topics

- **CxP Software and Autonomy Technology Needs,**
  - Presented by Ron Morillo
- **CxP Mission Operations Technology Needs**
  - Presented by Ernest Smith
- **CxP Integrated Build Tool Concepts**
  - Presented by Leslye Boyce
- **CxP Verification, Validation and Accreditation Concepts**
  - Presented by Randy Wallace

CxP Software and Autonomy Technology Needs

Ron Morillo
SAVIO Software
11/14/2007

Software technology drivers

- **The Constellation Program is interested in software technologies that support the following program objectives:**
  - Build safer software-intensive systems
    - Mitigate common cause failures
  - Reduce development and schedule risk
    - Manage the size and complexity of software interactions in all the phases of the life-cycle.
  - Improve fault detection, isolation and recovery techniques
  - Lower operational and maintenance cost.
  - Enable the move to greater on-board autonomy
    - Intelligent human-in-the-loop automation
  - Improve system performance analysis.
    - Timing, trending, forecasting

Specific SW technologies of interest - 1

- **Requirement Maturation:**
  - Ontology systems to determine precise meaning of requirements, avoid possible (mis)interpretations and determine completeness of the requirement set.
  - Requirement analysis for inconsistencies and contradictions
    - Many software-related mishaps, including common cause failures, trace back to incomplete or missing requirements

- **Design/Architecture:**
  - Capture the design knowledge once; use it to code, test and verify, operate the system
  - Physical and behavioral models that capture system properties, cause/effects, environment and interactions:
    - Quantify the complexity of SW code and interfaces
    - Improve model-based analysis and verification, testability and timing analysis.
  - Investigate the true bounds of dissimilar software design.
  - SW fault containment concepts.

Specific SW technologies of interest - 2

- **Autonomy and FDIR:**
  - Adjustable levels of autonomy and FDIR.
  - Technology for onboard Decision Support and Expert-guided troubleshooting to crew/ Ground.
  - Tie diagnostic/prognostic tools to on-board reconfiguration managers and/or intelligent controllers.
  - Within tight timing constraints:
    - Minimize false alarms, diagnosis ambiguity.
    - Detect trends
    - Assess failure severity for C&W.
  - Better forecasting capability (of system degradation, of remaining useful life, of impending failure..)
  - Re-planning following a failure:
    - Decompose high-level objectives onboard, incorporate locally determined information (situational awareness) and create an new execution plan.
  - When autonomy meets imperfect information: inductive reasoning techniques for managing certain degree of data inconsistency, limited knowledge or uncertain symptoms; models that manage imprecision and uncertainties

Specific SW technologies of interest - 3

- **SW implementation:**
  - Code analyzers and compliance rule checkers
  - Auto coding of critical software functions

- **SW Verification and Validation:**
  - Targeting specific tests towards mitigating specific classes or types of software defects.
  - Error injection, tracing and analysis technology
  - Model-based analysis for validation of safety-critical software designs.
  - Test suite generation, including behavioral coverage of safety-critical software functions.
  - Advanced Validation Testing that determines failure boundaries and margins for safety-critical functions.
  - Auto code tools for state estimation, data analysis and to streamline the test activity.
  - Verification and validation of autonomy and automation functions implemented in flight computers.

Specific SW technologies of interest - 4

- **Software reliability**
  - Quantifying the software risk contribution to the total risk in a system.
  - Modeling software failures.
  - Mature the technology of predictive SW/system reliability models validating these models with operational data.

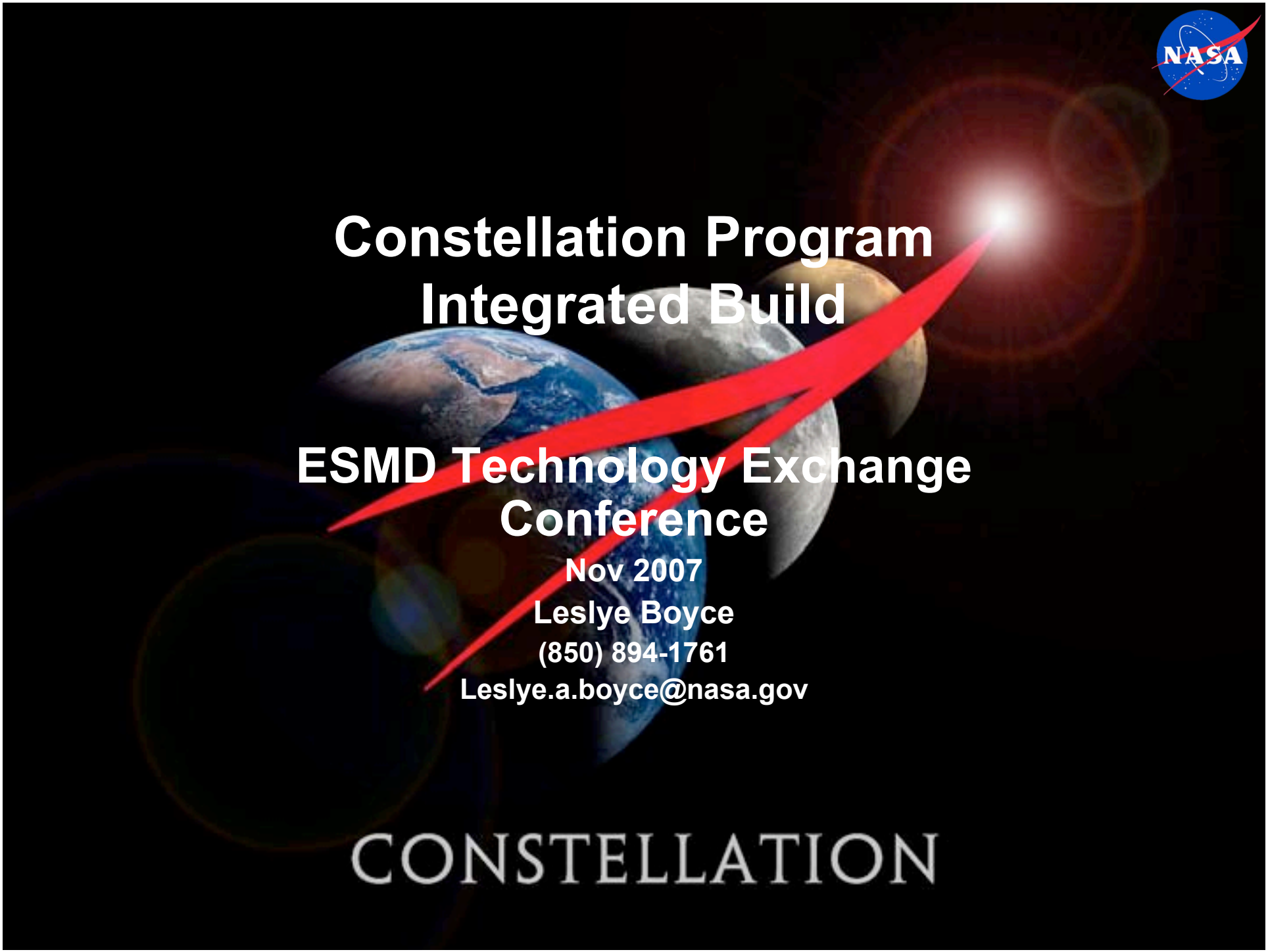
Mission Operations Overview For Technology Needs Assessment

Ernest Smith
Mission Operations Directorate

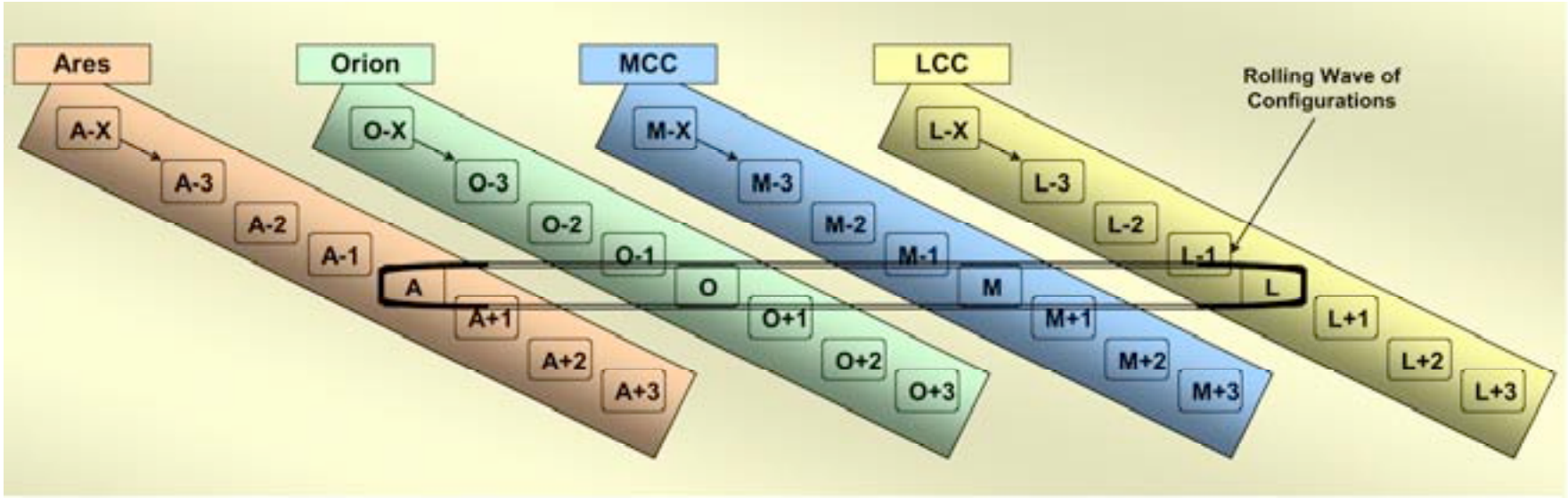
CONSTELLATION

Mission Operations Overview For
Technology Needs Assessment

- **Mission Operations at Johnson Space Center is preparing for our support to the Constellation Program**
  - Major mission operations systems upgrades/development include the Mission Control Center Systems, the Cx Training Facilities, Mission Ops Reconfiguration System, and Flight Design Applications
- **Technologies areas we require include those related to:**
  - Autonomy applications related to mission operations
  - Integrated Systems Health Monitoring tools
  - Software development tools (especially JAVA enterprise technology and Workflow tools)
  - Data mining/knowledge management
  - CFDP compatible tools for file transfers (CCSDS-based implementation of FTP)
  - Mission monitoring (telemetry and command) tools and applications
  - Scheduling tools
  - Training support applications and simulations technologies for both stand-alone part-task trainers and full capability simulations of vehicle systems
- **We have partnered with Ames for the past 2 years on technology infusion projects to enhance efficiency and capability associated with our plan/train/fly capabilities within Mission OPS, but are interested in other sources for technology infusion**

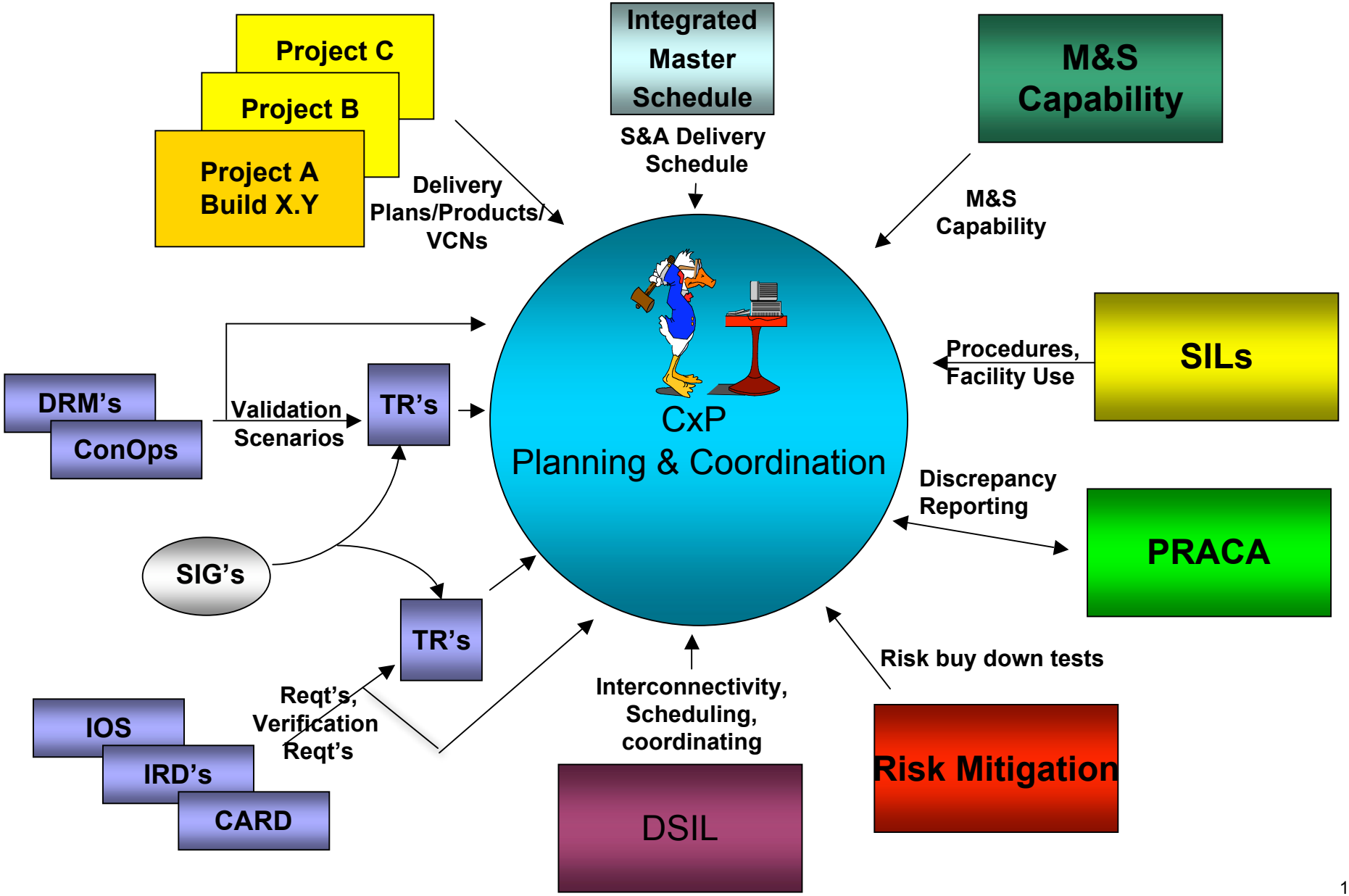

NASA
Constellation Program
Integrated Build
ESMD Technology Exchange
Conference
Nov 2007
Leslye Boyce
(850) 894-1761
Leslye.a.boyce@nasa.gov
CONSTELLATION

Phased Development Activities



- **CxP Integrated Software Planning is a complex task that requires a time phase approach and build up of capabilities**
  - Builds on multiple System Baselines as time phased capability is developed, integrated and verified (Qual. + Accept.)
  - Maintains & integrates multiple System Baselines during concurrent Architectural development
  - Provides Increment buildup of capability based on mission objectives
- **Key enablers for process include**
  - Planned – Phased Delivery of System Software from Projects
  - Reduction in Software Build Cycle Times to reduce risks
  - Identification and specification of Infrastructure Support Tools
  - Distributed, Early Interface Testing for design validation, risk reduction and Hardware/Software Integration

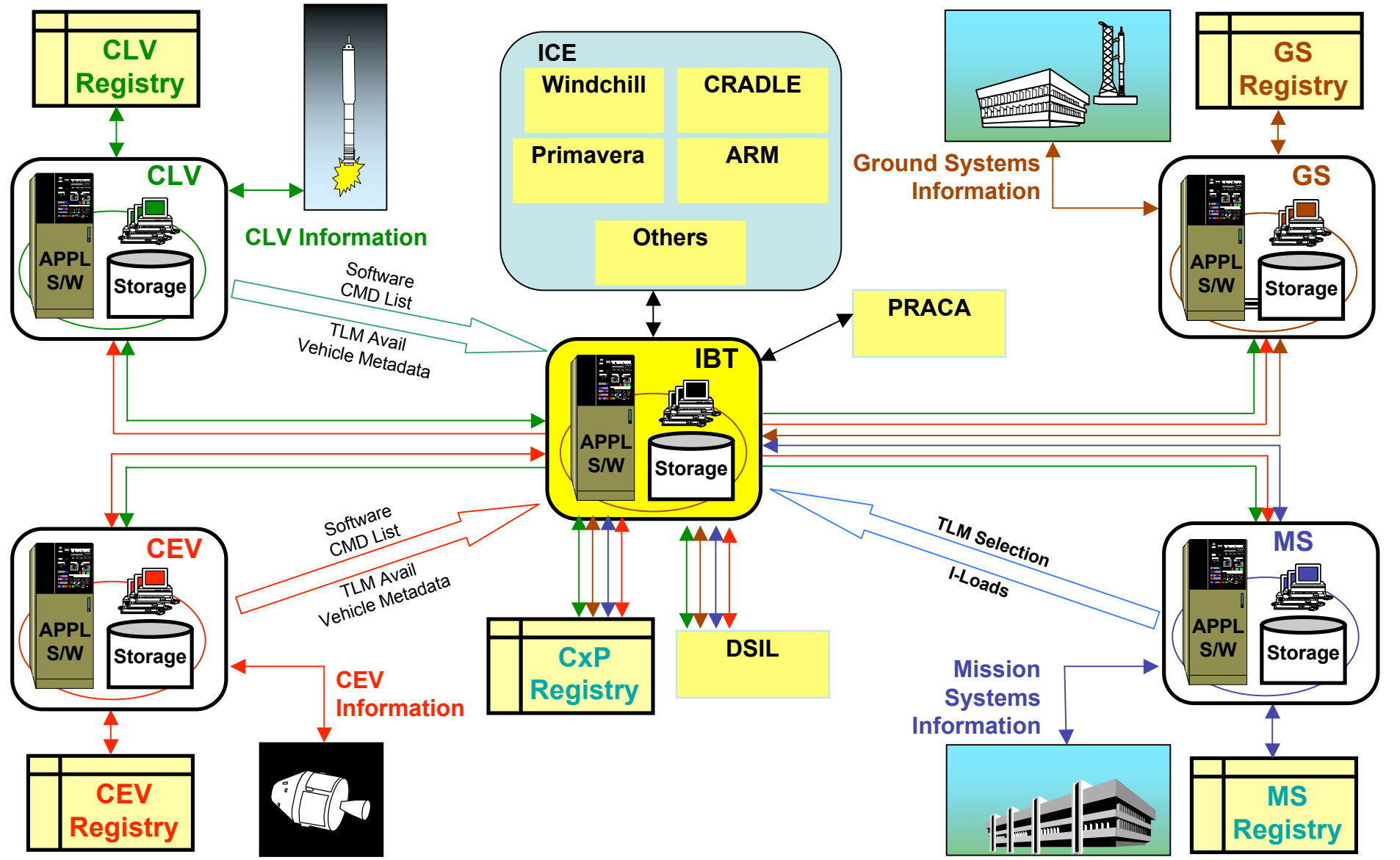
Verification and Validation Interactions



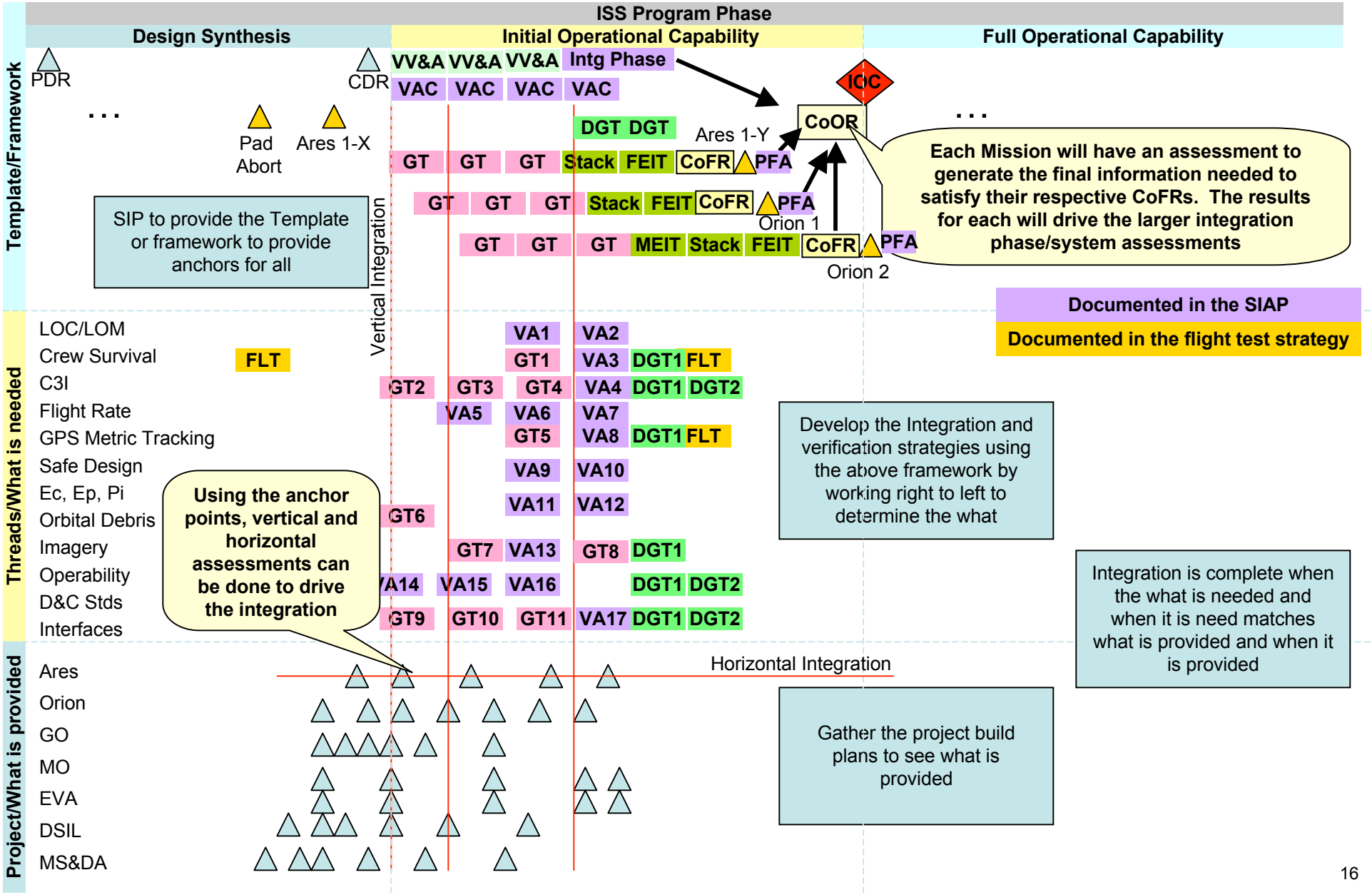
Requirements Highlights

- The IBT is the authentic source for all software, associated data and meta data for the CxP
- The IBT supports the planning, tracking, submittal, and distribution of software and data between the various Constellation projects and elements
- The IBT supports the decisions and manages the activities for the Computing Systems Control Panel as directed by the Constellation System Engineering Control Board
- The IBT supports the planning and tracking for System Integration Plan

Integrated Information Delivery



Desired End-State Captured in the SIP
Focused Look at ISS IOC - Draft



Modeling and Simulation Verification, Validation and Accreditation

ESMD Technology Exchange Conference

Nov 2007

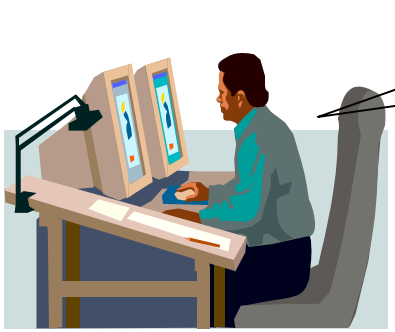
Randy Wallace
(256) 544-2940
Randal.L.Wallace@nasa.gov

CONSTELLATION

NASA M&S Environment

- Over 400 existing simulations
- Various conditions
- Numerous development efforts
- Over 700 identified needs for M&S
- Compressed schedules

M&S VV&A



Developer
Verification Agent

VERIFICATION

The process of determining that a model [or simulation] implementation and its associated data accurately represents the developer's conceptual description and specifications…***Did we build the thing right?***

Functional Expert
Validation Agent

VALIDATION

The process of determining the degree to which a model [or simulation] and its associated data provides an accurate representation the real world from the perspective of the intended uses of the model or simulation… ***Did we build the right thing?***

Requester/User
Accreditation Agent

ACCREDITATION

The official acceptance of a model or simulation or federation of models and simulations and its associated data to use for a specific purpose… ***Should it be used?***

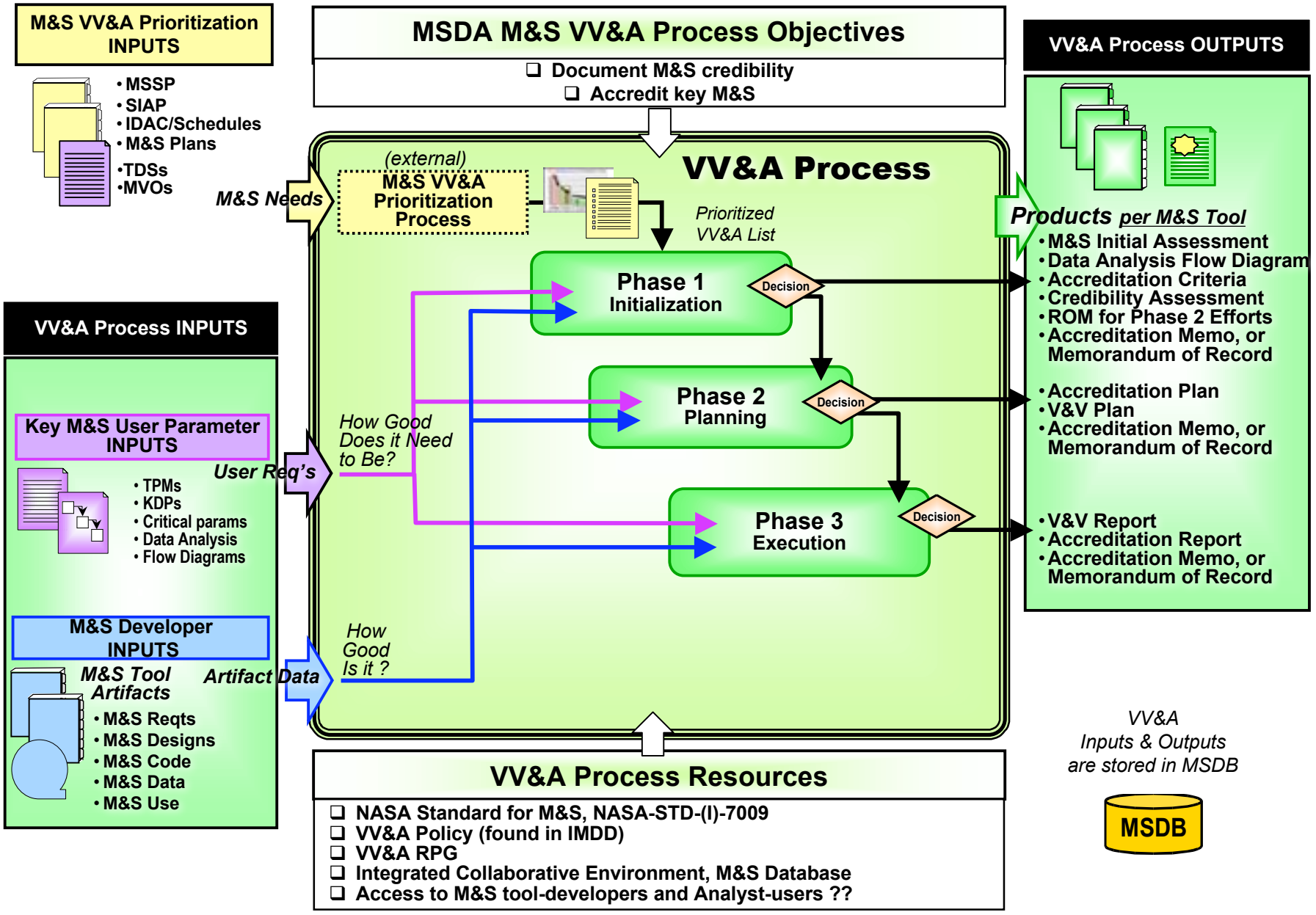
Verification, Validation, and Accreditation (VV&A):
A process for substantiating the credibility of models and simulations.

Benefits of VV&A

- Increase the credibility of M&S used.
- Supports NASA M&S Standard 70009
- Reduce the risks associated with the M&S used.
- Establish a solid understanding of M&S strengths and weaknesses, and the bounds within which they can credibly support decision-making.
- Ensure informed decision-making.
- Reliably realize the benefits of simulation

VV&A provides a mechanism to communicate credibility between M&S developers, analysts and decision makers

A Three Phased NASA Process



NASA M&S VV&A Needs

- Increased Awareness of VV&A requirements and applicability
- Tools to automate the verification process
- Consistent information management systems
- Real-world referent data on developmental systems
- Analysis Standards
- Analysis Recommended Practices Guide

The Fundamental Questions

Contact Information

- **Randy Wallace**
  - M&S VV&S Lead, CxP Software and Avionics Integration Office (SAVIO)
  - randal.l.wallace@nasa.gov
  - 256-544-2940
- **Lisa Caine**
  - Aegis Technologies
  - Lcaine@aegistg.com
  - 256-922-0802